Introduction To Intrusion Detection System: Review

Rajni Tewatia, Asha Mishra

Abstract: Security of a network is always an important issue. With the continuously growing network, the basic security such as firewall, virus scanner is easily deceived by modern attackers who are experts in using software vulnerabilities to achieve their goals. For preventing such attacks, we need even smarter security mechanism which act proactively and intelligently. Intrusion Detection System is the solution of such requirement. Many techniques have been used to implement IDS. These technique basically used in the detector part of IDS such as Neural Network, Clustering, Pattern Matching, Rule Based, Fuzzy Logic, Genetic Algorithms and many more. To improve the performance of an IDS these approaches may be used in combination to build a hybrid IDS so that benefits of two o more approaches may be combined.

Index Terms: Intrusion Detection system (IDS), Attack, Data, False alarm, Intruder, Network, Approach.

1 INTRODUCTION

At present network revolution is an essential part of communication. But with new trends of internet the threats to network is also increasing. The traditional devices such as firewall, virus scanner are in their limits to cope up with the growing number of intelligent attacks from the internet. An attack is a realization of threat to find and exploit the system vulnerability [6]. An intrusion detection system is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall. An intrusion detection system is a device typically a designated computer system that continuously monitors activity to identify malicious alerts. A single intrusion in a network can be reason of information leakage and can perform data modifications that are very harmful to any type of organization [7].

2 RELATED WORK

Dorothy E. Denning [1] proposed a model of real time intrusion detection expert system. The model is based on the hypothesis that exploitation of system's vulnerability involves abnormal use of the system. She provided a frame work for general purpose intrusion detection expert system which we have called IDES. She provided Statistical models like Operational Model, Mean and Standard Deviation Model, Multivariate Model, Markov Process Model and Time Series Model.

Nawal A. Elfeshawy and Osama S. Faragallah[2] gave the basic working of intrusion detection system and its characteristics. **THEY** also explain some approaches for developing IDS and a frame work investigation of intrusions.

- Rajni Tewatia is currently pursuing masters degree program in Computer Science and engineering in, BSAITM, Faridabad, Haryana, India rajnitewatia1057@gmail.com
- Asha Mishra is Senior Lecturer in Department of computer science & Engineering ,BSAITM, Faridabad, Haryana, India asha1.mishra@gmail.com

Shaik Akbar, Dr.K.Nageswara Rao, Dr.J.A.Chandula [3] Presented intrusion system methodologies based on data analysis. Different data analysis methodologies are explained for IDS.

Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslawszymanski, Mark Embrechts [4] Presented network based intrusion detection using neural network. It is modular network based intrusion detection system that analyzes data and some of its components must be trained such as SOM and NN.

Amit Kumar,Harish Chandra Maurya and Rahul Mishra[5] proposed a hybrid intrusion detection system. They used two classification technique for our proposed architecture, in combined manner. They combined Bayes' Therom, naïve Bayes Classifier for intrusion detection and K-means Clustering to detect intrusion.

3 INTRUSION DETECTION SYSTEM (IDS)

Intrusion detection is defined as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity availability or to bypass the security mechanism of computer or network [3].The main components of IDS are shown in Fig.1.

3.1 Components of Intrusion Detection System

- **Data Collection/Preprocessor**: Data collection component is responsible for collecting and providing the audit data that will be used by next component to make decisions. Data used for detecting intrusion ranges from user access pattern to network packet level features [5].
- **Analyzer (Intrusion Detector):** The analyzer or the intrusion detector is the core component which analyzes the audit patterns to detect attacks. This is a critical component and one of the most researched. Various techniques are used as intrusion detectors [5]
- **System profile (database or knowledge base):** The system profile is used to characterize the normal and abnormal behavior. It is the knowledge base for attacks, configuration information about the current state of the system and audit information describing the events that are happening on the system.

- **Response Engine:** The response engine controls the reaction mechanism and determines how to respond. The system may raise an alarm and report to administrator or may block the source of attack [5].

3.2 An Ideal IDS must do the following

- It must run continually without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed.
- It must be fault tolerant in the sense that it must survive a system crash and not lose its knowledge-base at restart.
- It must impose minimal overhead on the system.
- It must cope with changing system behavior over time as new applications are being added.

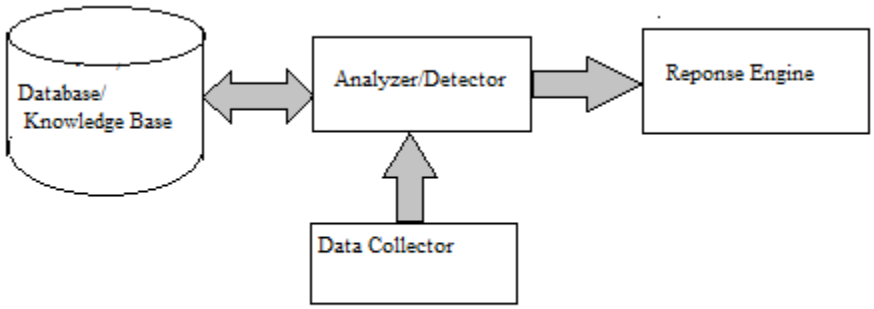

Fig.1 A Typical IDS with Its Components

3.3 Attacks which should be handled by IDS

In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of a source.

Denial of Service (DoS): A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests.

R2L(remote to local): A R2L attacks are exploitations in which the hacker starts off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges.

U2R(remote to user): A remote to user (U2R) attack is an attack in which a user sends packets to a machine over the internet, which he/she does not have access to in order to expose the machines vulnerabilities and exploit privileges which a local user would have on the computer.

Probes: A probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system.

4 CLASSIFICATION OF INTRUSION DETECTION SYSTEM

Intrusion Detection System can be classified into following categories as in Fig. 2.

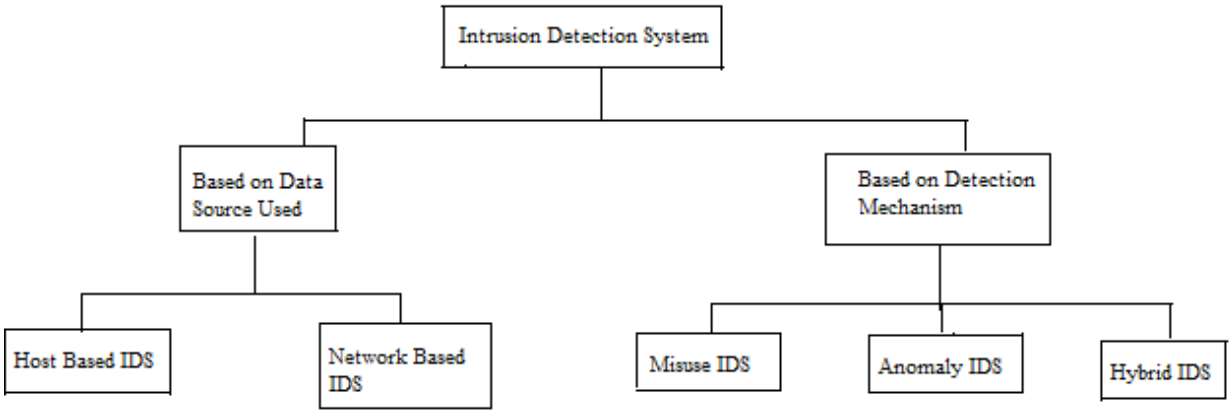

Fig.2. Classification of Intrusion Detection System

4.1 Host based intrusion detection:

A Host based IDS resides on the system being monitored. It consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file system modifications and other host activities and state.

4.2 Network Based Intrusion Detection:

A Network Based Intrusion Detection System monitors and analyzes the traffic on its network segment to detect intrusion attempts. Implementation for it requires

1. Network interface card to captures all traffic that goes through the network.
2. Sensor which monitors to determine if, packet flow matches with known signature [3].

4.3 Misuse Intrusion Detection System

This detection technique uses specifically known patterns to detect malicious code. These specific patterns are called as signatures. if current activity match with any of known signatures an alarm is triggered

Low Rate of False Alarms: The main advantage of misuse detection system is their ability to detect known attacks and the relatively low false alarm rate when rules are correctly defined.

Only Known Attacks: The foremost drawback of misuse detection system is their complete inability in detecting unknown attacks [3].

4.4 Anomaly Intrusion Detection System

These techniques are designed to detect abnormal behavior in the system. The normal usage pattern is base lined and alerts are generated when usage deviates from the normal behavior.

Unknown Attack Detection: The main advantage of anomaly detection system is that contrary to misuse detection system, they can detect unknown or novel attacks.

High Rate of False Alarms: Very high rate of false alarms leads to very poor accuracy of anomaly detection system [3].

4.5 Hybrid Intrusion Detection System

Early research works on intrusion detection systems suggested that the intrusion detection capabilities can be improved through a hybrid approach consisting of both signature (misuse) detection as well as anomaly detection. In such a hybrid system, the signature detection technique detects known attacks and the anomaly detection technique detects novel or unknown attacks.

Low False Rate: This technique reduces the large number of false alerts generated by current anomaly detection approaches [6].

5 OVERVIEW OF INTRUSION DETECTION APPROACHES

A brief overview review of these famous approaches is given below Fig.3 that are landmarks in the development of intrusion detection systems.

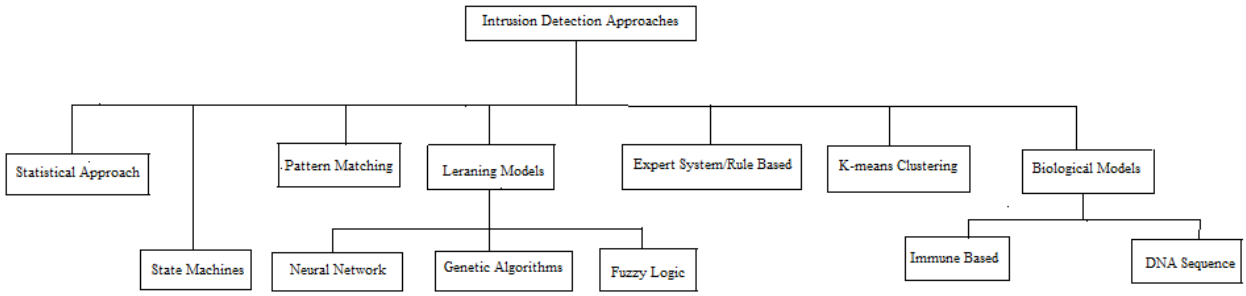

Fig.3 Intrusion Detection Approaches

5.1 Statistical Approach

This approach includes statistical comparison of specific events based on a predetermined set of criteria. The user or system behavior (set of attributes) is expressed as number of variables over time. Examples of such variables are user login, logout, number of files accessed in a period of time, usage of disk space, memory, etc [2]. The collected data was tested for attack analysis by statistical models.

5.2 Data Mining

Data mining techniques have been applied to network and host audit data for building misuse detection models. In this case, intrusion detection is considered as a data analysis process, in which data mining techniques are used to automatically discover and model features of user's normal or intrusive behaviors [6]. Data Mining commonly involves four classes of task [2]. Classification, Clustering, Regression, and Association rule learning.

5.3 Pattern Matching

Pattern matching based intrusion detection approaches are commonly used in the network based intrusion detection systems in which attack patterns are modeled, matched and identified based on the packet head, packet content or both. Attack patterns could also be established in host-based intrusion detection systems through concatenating the words representing the system calls in a system audit trail [6]. With the continual emerging of new types and varied forms of attacks the number of signatures is constantly growing, thus making the pattern matching more expensive in terms of the computational cost. This is also unable to detect new attacks.

5.4 Expert System/Rule Based

The expert system working principle is based on a previously defined set of rules describing an attack. All security related events incorporated in an audit trail are translated in terms of it-then-else rules [3]. Expert systems-

based IDSs build statistical profiles of entities such as users, workstations and application programs and use statically unusual behavior to detect intruders. Unfortunately, Expert Systems require frequent updates by a System Administrator to remain up to date. The lack of maintenance or update is the weakness of this approach [2].

5.5 State Machines

The state machines model is collection of states, transition and actions. An attack is described with a set of goals and transition that must be achieved by an intruder to compromise a system [3].

5.6 K-means Clustering

The k-means algorithm takes the input parameter k, and partitions a set of n objects into k clusters so that the resulting intra-cluster similarity is high but the inter-cluster similarity is low.. The main goal to utilize K-Means clustering approach is to split and to group data into normal and attack instances [5].

5.7 Learning Models

Learning models incorporate learning capabilities in intrusion detection process, using artificial leaning techniques. In recent years, learning techniques have been widely used in anomaly detection since the self-learning techniques can automatically form an opinion of what the subject's normal behavior is [6].

5.7.1 Using Neural Network

An early attempt for intrusion detection is using neural network, which consists of two components. The first component is an expert system, which monitors audit trails for known intrusion signatures. The second component uses neural network to learn user behaviors; it then fires an alarm when there is a deviation between current behaviors and learnt behaviors [6]. Neural network which are class of machine learning algorithms used to classify data. A neural network consists of nodes and edges. The values of weight on edge define how a node affects adjacent nodes. A subset of the nodes in the model is called input nodes, which there is no connection themselves.

Detection using neural networks is three-step process.
The first step consist of determining what kind of input data will be given and what output we want.
The second step consists in training the network that is mapping the input-output by adjusting weights of the edges. This is the learning phase of the method.
The third step consists in using this network to detect anomalies. Depending on the output of the network, we can determine whether the input vector was anomalous or not [3].

5.7.2 Fuzzy logic

Fuzzy logic is a form of many-valued logic that deals with approximate, rather than fixed and exact reasoning. Fuzzy set theory was introduced by Zadeh in 1965 and it was specially designed mathematically represent uncertainty and vagueness with formalized logical tools for dealing with impression inherent in many real world problems. The fuzzy logic based system could be able to detect various types of the intrusive activity of computer networks as the rule base holds a better set of rules[8].

5.7.3 Genetic algorithms

A genetic algorithm (GA) is a programming technique that uses biological evolution as a problem solving strategy. It is based on Drawinian's principle of evolution and survival of fittest optimizes a population of candidate solutions towards a predefined fitness. The proposed GA based intrusion detection system contains two modules where each works in a different stage, a set of classification rules are generated from network audit data using the GA in offline environment. In intrusion detection stage, the generated rules are used to classify incoming network connections in the real-time environment. GA uses evolution and natural selection that uses a chromosome-like data structure and evolve chromosomes using selection, recombination and mutation operator. From each chromosomes different position are encoded as bits, character or numbers. These positions could be referred to as gene[8]. However, the major limitation of this approach is that an improper threshold value might easily lead to a high false alarm rate in detecting new attacks [6].

5.8 Biological Models

Several anomaly detection models inspired from biological principles have been proposed in the literature.

5.8.1 Immune Based

The immune based IDS is based on human immune system concepts and can perform tasks similar to innate and adaptive immunity. The profile of normal behavior is generated by collecting appropriate behavior of services from audit data [4]. There is analogy between human immune system's capability of distinguishing self from nonself and intrusion detection system. When applying the self-nonself technique to intrusion detection, behaviors of the system are viewed as a string [6]

5.8.2 DNA Sequence

Another interesting biological method for intrusion detection proposed by Yu et al. is based on the DNA sequence Yu et al. define DNA sequences for a computer system based on the knowledge that the DNA characterizes the makeup of human body and that any anomaly in tissues can be reflected in a particular DNA sequence. Any change in the behavior patterns of the computer system may be traced to the change of DNA sequences that can be either normal or abnormal. A standard back-propagation neural network was used to train normal DNA sequences for network traffic [6].

6 Proposed Hybrid Approach

6.1 Analysis of Different Approaches:

This is done on the basis of analysis of the advantage of different approaches to introduce proposed approach as in Fig.4.

6.2 Clustering Advantages:

- Unsupervised learning technique
- Facilitate real-time detection
- Improved detection efficiency

6.3 Soft Computing Approach Advantages:

- supervised anomaly detection technique
- accurate detection
- Much better solution
- Better generalization abilities
- Faster processing time

The proposed hybrid approach gives better performance over individual approaches. The data instances include two clusters: intrusive cluster and normal cluster through the clustering algorithm and after that apply soft computing Approach to make system adaptive and automated because soft computing is a supervised approach that needs training of data.

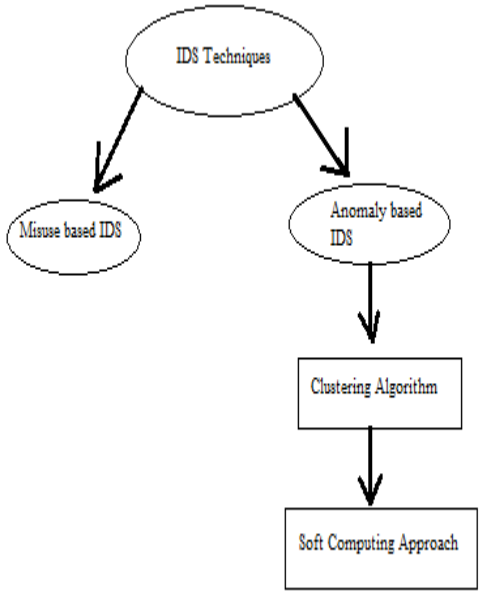

Fig.4 Proposed Hybrid Approach

7 CONCLUSION

The field of intrusion detection has been around since 1980's and a lot of advancement has been made in the same field. Many methods have been employed for intrusion detection. In this paper we discussed many approaches to implement the intrusion detection system. With the help of any of the above discussed techniques\approach algorithms may be designed so that network becomes safe and secure. This intrusion detection has to be done but not at the cost of system performance.

REFERENCES

[1] Dorothy E. Denning "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, vol.SE-13, No.2, February 1987.

[2] Nawal A. Elfeshawy and Osama S. Faragallah "Divided two part adaptive intrusion detection system", Published online: 13 June 2012 Springer Science+Business Media, LLC 2012.

[3] Shaik Akbar, Dr.K.Nageswara Rao, Dr.J.A.Chandula "Intrusion Detection System Methodologies Based on Data Analysis", international Jouranal of Computer Application(0975-8887) Volume 5-no.2, August 2010.

[4] Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslawszymanski, Mark Embrechts "Network-Based Intrusion Detection Using Neural Networks", Proc. Intelligent Engineering Systems through Artificial Neural Networks ANNIE-2002, St. Louis, MO, vol. 12, ASME Press, New York, NY, 2002, pp. 579-584.

[5] Amit Kumar,Harish Chandra Maurya and Rahul Mishra " A Research Paper on Hybrid Intrusion Detection System", International Journal and Advanced Technology(IJEAT) ISSN:2249-8958, Volume-2, Issue-4, April 2013

[6] Ghorbani, AA, Lu, W, Travallaee, M, "Network Intrusion Detection and prevention Concepts and Techniques "Springer 2010, hardcover, ISBN:978-0-387-88770-8

[7] Sharddha Surna "Intrusion Detection using Fuzzy Clustering and Artificial Neural Network", Advances in Neural Networks, Fuzzy Systems and Artificial Intelligence.

[8] Mostaque Md. Morshedur Hassan "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic" International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 7, September 2013.

[9] Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslawszymanski, Mark Embrechts "Network-Based Intrusion Detection Using Neural Networks" Proc. Intelligent Engineering Systems through Artificial Neural Networks ANNIE-2002, St. Louis, MO, vol. 12, ASME Press, New York, NY, 2002, pp. 579-584.